UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

SHON HENDERSON, on behalf of herself and all others similarly situated, Plaintiffs, v. **EQUIFAX, INC.**, Defendant.	CASE NO. **Jury Trial Demanded**

CLASS ACTION COMPLAINT

Plaintiff Shon Henderson, on behalf of herself and all others similarly situated, files this Class Action Complaint ("Complaint") against Defendant Equifax, Inc. ("Equifax"), a Georgia Corporation. Based on information and belief and investigation of counsel, Ms. Henderson alleges as follows:

INTRODUCTION

1. Equifax boasts: "We have built our reputation on our commitment to deliver reliable information to our customers, . . . and to protect the privacy and confidentiality of personal information about consumers. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax."

2. This claim on Equifax's "Privacy" webpage remains, even though Equifax's

failed data security allowed third parties to access the names, addresses, Social Security numbers, and other personally identifiable information ("PII") of over 140 million United States consumers—almost half the population of the United States.

3. Equifax also admits that credit card numbers for approximately 209,000 United States consumers were accessed, as was dispute documentation (that contained additional PII) for approximately 182,000 Unites States consumers. Since its initial disclosure, Equifax has admitted that credit card transaction history going back to November 2016, was also included for some affected individuals.

4. This data breach ("Breach") purportedly began in mid-May and ended on July 29, 2017, when Equifax finally realized its security had been compromised.[1]

5. While Equifax allegedly learned of the Breach on July 29, 2017, Equifax did not acknowledge the Breach nor inform the public until September 7, 2017, well over one month later. This delay, coupled with Equifax's decision to apparently announce the data breach after the end of the trading day (and after several of its executives unloaded some stock worth approximately $2 million), belies Equifax's claim that it began notification as soon as it had enough information to do so.

6. To make matters worse, Equifax has since revealed the true cause of the

---

[1] The California Attorney General's website indicates the Breach took place May 13, 2017 – July 30, 2017. Submitted Breach Notification Sample, available at: https://oag.ca.gov/ecrime/databreach/reports/sb24-101693.

Breach: a well-publicized and patchable vulnerability in the open source software, Apache Struts. Equifax claims that it engaged an independent cybersecurity firm to conduct a comprehensive forensic review. Despite that, and despite having five weeks from discovery to public notification, Equifax's initial disclosures were vague, referencing a "U.S. website application vulnerability."[2] Equifax waited an additional week before revealing the root cause of the security breach, which turned out to be entirely preventable.

7. More damningly, Equifax acknowledged the following day that it had been aware of the vulnerability and the patch in early March 2017.[3] Equifax could have prevented the Breach entirely had it updated its software when notice of the patch went out in March 2017—some two months before Equifax claims the Breach started.[4]

8. The Breach followed other recent Equifax security breaches that exposed the Social Security numbers and other PII of thousands of individuals. These prior events

---

[2] Cybersecurity Incident & Important Consumer Information (Consumer Notice), Equifax Security 2017, https://www.equifaxsecurity2017.com/consumer-notice/.

[3] Press release, "Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes," Equifax Investor Relations (Sept. 15, 2017), https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832.

[4] Brian Krebs, "Equifax Hackers Stole 200k Credit Card Accounts in One Fell Swoop," KrebsOnSecurity (Sept. 14, 2017), https://krebsonsecurity.com/2017/09/equifax-hackers-stole-200k-credit-card-accounts-in-one-fell-swoop/.

should have provided Equifax advance warning of its data security shortcomings, yet Equifax still failed to adequately safeguard consumers' PII, creating a massive threat to those whose PII was improperly safeguarded.

9. Not only that, but, two weeks after its initial disclosure of the Breach, Equifax confirmed that it had experienced yet another security incident earlier in the year, before the Breach, telling NPR that, "during the 2016 tax season, Equifax experienced a security incident involving a payroll-related service."[5] Equifax failed to shore up its security before the Breach despite repeatedly being put on notice that its security was wholly inadequate.

10. Many in the security industry are calling this the worst data breach in the history of the United States, and criticize Equifax for arguably the worst data breach response ever.[6]

---

[5] Merrit Kennedy, "Equifax Confirms Another 'Security Incident,'" NPR (Sept. 19, 2017, 9:46 p.m.), http://www.npr.org/sections/thetwo-way/2017/09/19/552124551/equifax-confirms-another-security-incident; *see also* Michael Riley, Anita Sharpe, and Jordan Robertson, "Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed," Bloomberg Technology (Sept. 18, 2017, 2:55 p.m.), https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed ("The revelation of a March breach will complicate the company's efforts to explain a series of unusual stock sales by Equifax executives.").

[6] See e.g., Dan Goodin, "Why the Equifax breach is very possibly the worst leak of personal info ever," arstechnica (Sept. 7, 2017, 11:09 p.m.) https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/; Maria Aspan, "Why Equifax's

11. Senator Mark Warner (D-Va.), who heads the bipartisan Senate Cybersecurity Caucus, stated that "it is no exaggeration to suggest that a breach such as this – exposing highly sensitive personal and financial information central for identity management and access to credit – represents a real threat to the economic security of Americans."[7]

12. Senate Minority Leader Chuck Schumer (D-NY) criticized Equifax's "disgusting" treatment of consumers. "It's one of the most egregious examples of corporate malfeasances since Enron," said Schumer.[8]

13. This Complaint is filed on behalf of all persons who were victimized by the Breach, as more fully described herein. As a result of Equifax's willful failure to prevent the Breach, Plaintiff and the Class are far more likely to suffer from identity theft and financial fraud, including fraudulently filed tax returns, fraudulent transactions on existing lines of credit, obtaining government benefits in a victim's name, and the creation of fraudulent financial accounts opened in their names, among

---

Response Makes Its Data Breach the Worst Ever," Inc. (Sept. 8, 2017), https://www.inc.com/maria-aspan/equifax-data-breach-worst-ever.html.

[7] Lee Mathews, "Equifax Data Breach Impacts 143 Million Americans," Forbes (Sept. 7, 2017, 10:42 p.m.), https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#63b34883356f.

[8] Dustin Volze, Susan Heavey, "FTC probes Equifax, top Democrat likens it to Enron," Reuters (Sept. 14, 2017, 6:48 a.m.), https://www.reuters.com/article/us-equifax-cyber-ftc/ftc-probes-equifax-top-democrat-likens-it-to-enron-idUSKCN1BP1VX.

myriad other risks. Due to these risks, the victims of the Breach will have to pay for credit monitoring and identity theft protection services far more than one year into the future, and many will seek such services from a company other than the one that exposed their information in the first place. Ultimately, victims of the Equifax breach have devoted and will continue to devote significant time, money, and energy into safeguarding and monitoring their PII and the accounts linked to it for years to come.

JURISDICTION AND VENUE

14. This Court has original subject matter jurisdiction of this action under the Class Action Fairness Act of 2005. Pursuant to 28 U.S.C. §§ 1332(d), and 28 U.S.C. § 1348, this Court has original jurisdiction because the aggregate claims of the members of the proposed Classes exceed $5 million, exclusive of costs, and at least one of the members of the proposed Classes is a citizen of a different state than Equifax. Further, there are far more than 100 members of the proposed Classes nationwide.

15. This Court has personal jurisdiction over Equifax because Equifax maintains its principal place of business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts with Georgia. Equifax avails itself of this jurisdiction by marketing and selling its products and services from this District to millions of consumers nationwide.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Equifax's

principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

THE PARTIES

17. Plaintiff Shon Henderson is a resident of Benicia, California.

18. Plaintiff Henderson paid $10 to Equifax for a credit freeze in October 2016. She trusted Equifax would protect her personally identifiable information. Following the announcement of the Breach, she entered her information into the page Equifax established for consumers. The page indicated she "may have been impacted by this incident." The information that may have been compromised includes her name, Social Security number, birth date, address, and potentially other information. As a result, Plaintiff Henderson has spent time and effort monitoring her financial accounts in the wake of the public announcement of the Breach.

19. Defendant Equifax, Inc. is a corporation organized under the laws of Georgia and headquartered in Atlanta, Georgia.

FACTUAL ALLEGATIONS

A. The Breach compromised the PII of over 140 million U.S. consumers

20. On September 7, 2017, apparently after the close of the trading day, Equifax announced to the world that it had suffered a breach that exposed the names, Social Security numbers, birth dates, addresses, and in some instances, drivers' license

numbers of over 140 million United States consumers. In addition, Equifax admitted that credit card numbers for approximately 209,000 customers were breached, and dispute documentation for approximately 182,000 customers was also accessed, which included additional PII.

21. Equifax claims that it discovered the Breach on July 29, 2017. Equifax claims that the Breach began in mid-May 2017, and remained undetected for almost three months until Equifax's alleged discovery on July 29.

22. After discovery, Equifax waited over a month before disclosing the Breach, which lawmakers are calling "unprecedented" and "a real threat to the economic security of Americans." While Equifax claims it began notification as soon as it had enough information to do so, its preparations left 143 million consumers in the lurch with their most sensitive information exposed.

23. Perhaps more troubling is that Equifax executives, including the Equifax Chief Financial Officer, the President of U.S. Information Solutions, and the President of Workforce Solutions, made unscheduled transactions selling hundreds of thousands of dollars in Equifax stock mere days after the Breach was discovered, but about a month before Equifax made the news public. For example, John Gamble, Equifax's Chief Financial Officer, sold shares worth over $946,000. Yet, Equifax has claimed that these high-level executives had no knowledge of the breach. So, either Equifax is so

poorly run that its CFO was not told about a massive data breach that exposed very sensitive information of over 100 million U.S. residents, or its CFO defrauded the securities market.

B. Equifax waited another week before disclosing it could have easily prevented the Breach

24. On September 13, 2017, Equifax confirmed what security researchers already suspected in an update to its breach disclosure:

> Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638.[9]

25. Apache Struts is a popular open source framework used to develop Java-based apps. Its users include governmental agencies, Fortune 500 companies, Experian (another credit reporting agency), and annualcreditreport.com, the website provided for by the federal government for annual free credit checks.

26. Troublingly, the Apache Struts CVE-2017-5638 vulnerability was detected—

---

[9] "A Progress Update for Consumers, Equifax Security 2017 (Sept. 13, 2017), https://www.equifaxsecurity2017.com/2017/09/13/progress-update-consumers-4/.

and *patched*—months before Equifax alleges the Breach *began*. Security researchers identified the so-called "zero day" vulnerability in early March 2017. Apache Struts had released a patch by March 8, 2017.[10] The National Vulnerability Database, hosted by the U.S. National Institute of Standards and Technology, had a detailed page on the vulnerability posted on March 10, 2017, with links to analysis and patch information.[11]

27. The patch was provided free of charge, and security researchers went to great lengths to publicize it. All Equifax had to do was update its systems. Apparently, it did not.

> This would be not unlike a security guard notifying the head of bank security that the bank vault was being left unlocked night after night, and the head of security kind of just ignoring it. Surprise: the bank was eventually robbed. Except, at this bank, the transactions are done with your personal data. It's completely irreplaceable.[12]

28. Equifax even admits it knew of the patch back in March 2017. Had Equifax

---

[10] Brian Krebs, "Equifax Hackers Stole 200k Credit Card Accounts in One Fell Swoop," KrebsOnSecurity (Sept. 14, 2017), https://krebsonsecurity.com/2017/09/equifax-hackers-stole-200k-credit-card-accounts-in-one-fell-swoop/. Screenshots for both annualcreditreport.com and Experian, showing the vulnerability, were publicly posted the same week.

[11] "CVE-2017-5638 Detail," National Vulnerability Database (original release March 10, 2017; last revised August 15, 2017), https://nvd.nist.gov/vuln/detail/CVE-2017-5638.

[12] Kelly Mears, "Equifax Finally Explains How They Got Hacked," The Other98 (September 14, 2017), https://other98.com/equifax-finally-explains-got-hacked/.

properly deployed the patch when it was first released, it is likely the Breach would have been prevented.[13]

C. Equifax experienced prior data breaches and owns identity protection services, yet failed to implement adequate safeguards to protect PII

29. As one of the three largest credit bureaus in the United States, Equifax is believed to have PII in its possession on over 800 million individuals worldwide. Equifax's business model revolves around buying, selling, collecting, and storing consumers' PII for financial gain.

30. Due to Equifax's relatively unique position as a purveyor of such a massive amount of PII, Equifax also owns and operates a number of credit-related services, including an identity theft protection and credit monitoring service, called TrustedID, which uses Equifax's vast PII database to attempt to monitor for fraud.

31. The other two major credit bureaus, Experian and Transunion, have similar services, called ProtectMyID and TrueIdentity, respectively. Due to the nature of their business, these larger credit bureaus know, or have every reason to know, the value of the PII they possess, and the importance of creating safeguards to protect consumers' PII from exposure and misuse.

---

[13] Press release, "Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes," Equifax Investor Relations (Sept. 15, 2017), https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832.

32. PII is valuable and thus is a frequent target of hackers. As such, in recent years many large companies and aggregators of PII have suffered data breaches, including Adobe, LinkedIn, eHarmony, MySpace, Snapchat, Friend Finder Network, Anthem, and Yahoo (multiple times), among others.

33. These breaches were extremely well-publicized, and should have put Equifax on alert to the prevalence of such breaches and that formidable data security policies and practices were warranted.

34. Equifax has had every reason to know of the risks associated with—and value of—stored PII. In the wake of some of the breaches listed above, the companies at fault would sometimes turn to Equifax to provide credit monitoring services to the harmed individuals.

35. Further, Equifax itself suffered data breaches as recently as May 2016 and March 2017, when W-2 forms for thousands of employees of the Kroger stores or Allegis Group, Inc., were stolen from other websites operated by Equifax or one of its wholly owned subsidiaries.

36. "I am troubled by this attack—described as 'one of the largest risks to personally sensitive information in recent years'—and by the fact that it represents the third recent instance of a data breach of Equifax or its subsidiaries that has endangered American's personal information," Senator Elizabeth Warren wrote in a letter to

Equifax's then chairman and chief executive, Richard Smith.

37. To put the value of PII into context, the 2013 Norton Report, based on one of the largest consumer cybercrime studies ever conducted, estimated that the global price tag of cybercrime is around $113 billion, with the average cost per victim being $298 dollars.

38. In the wake of the Breach, Equifax's CEO, Richard Smith, was forced to retire, but nevertheless, may ultimately collect as much as $90 million in compensation for his time at the helm of Equifax.[14]

39. Between being in the business of identity protection, and the multitude of well-publicized data breaches, including its own, Equifax had significant notice that it needed to maintain adequate security measures to insure the security of Plaintiff's PII, yet Equifax failed to do so.

40. Even the scope and severity of this Breach has seemingly not awakened Equifax to the very real dangers of failing to secure PII. On September 12, 2017, Brian Krebs explained that another security researcher had discovered a serious vulnerability in Equifax's South American operations:

> It took almost no time for them to discover that an online portal designed to let Equifax employees in Argentina manage credit report

[14] Jen Wiecnzer, "Equifax CEO Richard Smith Who Oversaw Breach to Collect $90 Million," Fortune (Sept. 26, 2017), http://fortune.com/2017/09/26/equifax-ceo-richard-smith-net-worth/

> disputes from consumers in that country was wide open, protected by perhaps the most easy-to-guess password combination ever: "admin/admin."
>
> …[A]ll employee passwords were the same as each user's username. Worse still, each employee's username appears to be nothing more than their last name, or a combination of their first initial and last name. In other words, if you knew an Equifax Argentina employee's last name, you also could work out their password for this credit dispute portal quite easily.
>
> But wait, it gets worse. From the main page of the Equifax.com.ar employee portal was a listing of some 715 pages worth of complaints and disputes filed by Argentinians who had at one point over the past decade contacted Equifax via fax, phone or email to dispute issues with their credit reports. The site also lists each person's DNI — the Argentinian equivalent of the Social Security number — again, in plain text. All told, this section of the employee portal included more than 14,000 such records.[15]

41. Equifax failed to take proper precautions before the Breach—the basic act of keeping its web applications updated—and it appears the Breach and associated reputation damage have not inspired Equifax to change its woeful approach to security.

D. The Breach has exposed Plaintiff and other consumers to a heightened, imminent risk of identity theft and fraud, and the TrustedID service offered is inadequate to protect against this risk

---

[15] Brian Krebs, "Ayuda! (Help!) Equifax Has My Data!" KrebsOnSecurity (Sept. 12, 2017), https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/. Equifax took down the portal after being contacted by KrebsOnSecurity.

42. Plaintiff and Class members are at a heightened, imminent risk of identity theft and fraud as result of their PII getting into the hands of malicious third-parties.

43. In response to this heightened, imminent risk of identity theft and fraud, Equifax is offering 12-month subscriptions for one year of its identity theft product, TrustedID Premier.

44. Unfortunately, the TrustedID service being offered is wholly inadequate to address the injuries Plaintiff and Class members have and will face.

45. TrustedID is a wholly owned subsidiary of Equifax that is believed to be operated by Equifax. Given that it was Equifax's flawed data security and practices that led to Plaintiff's injuries in the first place, the TrustedID service does not promote confidence. Plaintiffs and Class members must not be asked to trust Equifax to solve the very problem it caused. In the words of data security journalist Brian Krebs, "the fact that the breached entity is offering to sign customers up for its own identity protection services strikes me as pretty rich."

46. Even if TrustedID were not owned and operated by Equifax, Equifax offers an inadequate and insufficient remedy for its failure to adequately protect and secure Plaintiff's and Class members' PII. The subject service has a history of consumer complaints about its inability to actually detect identity theft, as well as the difficulty in obtaining customer service. Many customers and reviewers have suggested that

customer service is only available by phone for limited hours Monday through Friday.

47. As an illustrative example from less than a month before the Breach was announced, on August 22, 2017, a TrustedID consumer on ConsumerAffairs.com reported:

> I have paid for years of service. I figured out, not TrustedID, who is supposed to monitor these things, that my identity had been stolen. I immediately called TrustedID to help me with the identity theft only to find out their 'fraud' department is only open Monday-Friday. After waiting for their fraud department to open on Monday morning I called. They passed me on to the 'fraud' department, which turned out to be a foreign call center who had no idea who I was or why I was forwarded to them. The 'fraud' department (really a foreign call center) proceeded to ask for all my information like my social security number etc., which was what had just been stolen so why would I give it to some random person in a foreign call center who didn't work for TrustedID and did not know why I was forwarded to them. I have tried for 3 days now to get help or for someone to help walk me through the identity theft issue and how to proceed only to figure out there truly is no 'fraud' department for TrustedID and there is no credit 'disputes' department either. You are on your own if you encounter identity theft while being a TrustedID customer. They are completely useless and they don't seem to care."

48. Even if TrustedID were an adequate identity protection service, it stands to reason that an influx of ***half the population of the United States*** will further degrade the accessibility and quality of identity theft and credit monitoring services of TrustedID, rather than improve them.

49. The limited amount of protection—one year—offered through TrustedID further exacerbates the problem, as many identity thieves will wait years before

attempting to use the personal information they have obtained, especially when it comes to Social Security numbers, which are burdensome to change.

50. In particular, a Government Accountability Office ("GAO") study found that "stolen data may be held for up to a year or more before being used to commit identity theft." In order to protect themselves, Plaintiff and Class members will need to remain vigilant against unauthorized data use for years and decades to come.[16]

E. Equifax was required to ensure the security of Plaintiff's PII and to timely detect and provide notification of data breaches under federal and state law, but negligently failed to do so

51. The Breach was the direct and proximate result of the Equifax's failure to properly safeguard Plaintiff's and Class members' PII from exposure as required by state and federal laws and regulations, including the Gramm-Leach-Bliley Act ("GLBA"), and the California Consumer Records Act, among others.

52. Specifically, the GLBA imposes upon "financial institutions" "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." *See* 15 U.S.C. § 6801.

---

[16] "Report to Congressional Requesters," p. 33, Government Accountability Office (June 2007), www.gao.gov/new.items/d07737.pdf.

53. For purposes the GLBA, "non-public personal information" means personally identifiable financial information—

(i) Provided by a consumer to a financial transaction;

(ii) Resulting from any transaction with the consumer or any service performed by the consumer; or

(iii) Otherwise obtained by the financial institution. *See* 15 U.S.C. § 6809(4).

54. To satisfy this obligation, financial institutions must satisfy certain standards relating to administrative, technical, and physical safeguards:

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. *See* 15 U.S.C. § 6801(b).

55. In order to satisfy its obligations under the GLBA, Equifax was also required to "develop, implement, and maintain a comprehensive information security program" that, among other requirements, identifies "reasonably foreseeable internal and external risks to security, confidentiality, and integrity of consumer information that

could result in unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks." *See* 16 C.F.R. § 314.4.

56. Further, under the Interagency Guidelines Establishing Information Security Standards related to the GLBA, 12 C.F.R. Pt. 225, App. F, financial institutions have an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id.*

57. In addition, the Interagency Guidelines provide that "[w]hen a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible." *See* 12 C.F.R. Pt. 225, App. F.

58. For purposes of the GLBA, Equifax is a financial institution, and is therefore subject to its provisions. Equifax admits as much in its filings with the Securities and Exchange Commission.[17]

---

[17] *See* Equifax, Inc. 2016 10-K Report, ("We are subject to various GLBA provisions,

59. For the purposes of the GLBA, Plaintiff's and Class members' PII is both "nonpublic personal information" and "sensitive customer information."

60. If Equifax had developed, implemented, and maintained a comprehensive information security program as required by 16 C.F.R. § 314.4—that is, complied with the law—Plaintiff's and Class members' PII would not have been accessible to unauthorized persons.

61. In the wake of the Breach, a number of claims calling Equifax's anomalous and insufficient data security policies into question have come to light. For example, one consumer stated that, months prior to the Breach, the consumer complained to Equifax that an unencrypted "forgotten password e-mail" with a plaintext password had been delivered to the customer's recovery e-mail address without the customer actually requesting it. To the extent that passwords are being stored in plaintext, Plaintiff's and the Class members' PII is at an even higher risk due to such an inadequate data security process.

62. Equifax, despite having known of the Breach for more than a month before notifying anyone publicly, put forth a shoddy notification site that further confused the

---

including rules relating to the use or disclosure of the underlying data and rules relating to the physical, administrative and technological protection of non-public personal financial information."), https://www.sec.gov/Archives/edgar/data/33185/000003318517000008/efx10k20161231.htm.

issues. Equifax's breach-related site (equifaxsecurity2017.com), where consumers were entering six-digits of their Social Security numbers, had the administrator's credential information publicly available, a simple registration issue that should have been dealt with before the site went live. Many consumers' browsers flagged the site as "malicious" because of various security certificate issues, meaning their browsers would display a warning message in lieu of the page because the browsers detected problems with the site. Not only that, but various people have demonstrated that the page will give different results for the same information when accessed on a different device (e.g., mobile vs. desktop), and will even tell fictitious people they may have been affected, (e.g., "Smith" and "123456").

63. Astonishingly, in the wake of the Breach, some Equifax customer service representatives have been directing consumers to the wrong website via Twitter, erroneously sending consumers to "securityequifax2017.com" instead of "equifaxsecurity2017.com" and putting them at extreme risk of inputting information into a phishing website run by scammers.[18]

---

[18] Dell Cameron, "Equifax Has Been Sending Consumers to a Fake Phishing Site for Almost Two Weeks," Gizmodo (Sept. 20, 2017, 11:03 a.m.), https://gizmodo.com/equifax-has-been-sending-consumers-to-a-fake-phishing-s-1818588764. Luckily, that particular domain is owned by a good Samaritan who has posted a warning about security and phishing rather than preying on affected consumers.

64. It would not be the first time Equifax has used extremely insecure data security practices. In the aforementioned May 2016 breach of Equifax's W-2Express website relating to Kroger, third-parties were able to access W-2 data, including Social Security numbers, merely by entering the date of birth and last four digits of an employee's Social Security number.

65. Further, until very recently, Equifax was searching for someone to fill the vacant position of Vice President of Cybersecurity, the equivalent of chief information security officer, according to Equifax.

66. Equifax failed to develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems, in violation of 12 C.F.R. Pt. 225, App. F. Equifax also failed to notify individuals affected by the Breach, whose nonpublic personal information or sensitive customer information was exposed, as soon as possible, or in a timely and adequate manner.

67. The California Consumer Records Act requires that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably

believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay . . .” *See* Cal. Civ. Code § 1798.82(a).

68. For the purposes of the Consumer Records Act, Equifax is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82.

69. Under the Consumer Records Act, Equifax must “implement and maintain reasonable security procedures and practices appropriate to the nature of the information [and] to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.” Cal. Civ. Code § 1798.81.5(b).

70. Plaintiff’s and the California Subclass members’ PII (including but not limited to names, addresses, and Social Security numbers) includes personal information covered by Cal. Civ. Code § 1798.81.5(d)(1).

71. Because Equifax reasonably believed that Plaintiff’s and the California Subclass members’ personal information was acquired by unauthorized persons during the Breach, it had an obligation to disclose the Breach in a timely and accurate fashion under Cal. Civ. Code § 1798.82(a).

72. Equifax failed to disclose the Breach in a timely and accurate manner, in violation the Consumer Records Act.

73. Further, Equifax's requirement that consumers surrender legal rights against Equifax's wholly-owned subsidiary to use Equifax's TrustedID service, is a violation of the Consumer Records Act requirement that any identity theft prevention and mitigation service "shall be provided at no cost." *See* Cal. Civ. Code § 1798.82(d)(E)(2)(G). Equifax claims that it is exempting Breach-related TrustedID enrollees from waiving any legal rights, but it is unclear whether the terms of service adequately address this contention.[19]

74. Ultimately, Plaintiff's and Class members' injuries are a direct and proximate result of Equifax's failure to provide adequate security for Plaintiff's and Class members' PII, and Equifax's violation of applicable state and federal laws and regulations.

TOLLING

75. Equifax's knowing and intentional failure to disclose the Breach until September 7, 2017, tolled the commencement of any applicable statute of limitations to Plaintiff's and the Class members' claims until that date at the earliest.

---

[19] In response to public outcry, Equifax "quietly removed" certain information from its terms over the weekend. Paul Blumenthal, Arthur Delaney, "Equifax Is Trying To Make Money Off Its Massive Security Failure," Huffington Post (Sept 8, 2017, last updated Sept. 11, 2017), http://www.huffingtonpost.com/entry/equifax-breach-2017_us_59b2dae8e4b0b5e531062976.

CLASS ALLEGATIONS

76. Plaintiff brings this action on behalf of herself and the members of the proposed Classes under Rule 23(a), (b)(2), (b)(3), and/or (c)(4) of the Federal Rules of Civil Procedure. Plaintiff seeks to represent the following Classes:

A. Nationwide Class

77. Plaintiff brings her Stored Communications Act, negligence, and negligence *per se* claims on behalf of a proposed nationwide class ("Nationwide Class"), defined as follows:

> All persons in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach publicly announced by Equifax, Inc. on September 7, 2017.

B. California Subclass

78. Plaintiff brings her Unfair Competition Law and Consumer Record Act claims on behalf of a proposed California subclass ("California Class"), defined as follows:

> All persons in the State of California whose personally identifiable information was acquired by unauthorized persons in the data breach publicly announced by Equifax,

Inc. on September 7, 2017.

79. Plaintiff also brings her negligence claim (Second Cause of Action) separately on behalf of the California Class, in the alternative to bringing that claim on behalf of the Nationwide Class.

80. Except where otherwise noted, “the Class” and “Class members” shall refer to members of the Nationwide Class and the California Class, collectively.

81. Plaintiff reserves the right to redefine the Classes prior to class certification, after having the opportunity to conduct discovery and further investigation.

82. Plaintiff reserves the right to establish additional subclasses as appropriate.

83. Excluded from the Classes are Equifax, its parents, subsidiaries, affiliates, officers and directors, and any entity in which Equifax has a controlling interest.

84. **Numerosity.** Fed. R. Civ. P. 23(a)(1). The Class members are so numerous that joinder is impractical. The Classes consist of over 140,000,000 members; the precise number is within the knowledge of Equifax and can be ascertained by discovery and review of Equifax’s records.

85. **Commonality.** Fed. R. Civ. P. 23(a)(2) and (b)(3). There are numerous questions of law and fact common to the Class members, which predominate over any questions affecting only individual Class members. Common questions of law and fact include, but are not limited to:

(a) Whether Equifax engaged in the wrongful conduct alleged herein;

(b) Whether Equifax owed a duty to Plaintiff and the Class members to adequately protect their PII;

(c) Whether Equifax breached its duties to protect the personal information of Plaintiff and Class members;

(d) Whether Equifax knew or should have known that its data security systems and processes were vulnerable to attack;

(e) Whether Equifax violated the Stored Communications Act;

(f) Whether Equifax engaged in deceptive, unfair, unlawful and/or fraudulent business practices under California law;

(g) Whether Equifax's conduct violated the California Unfair Competition Law, Bus. & Prof. Code § 17200 *et seq.*;

(h) Whether Equifax unreasonably delayed in notifying California residents under the Consumer Records Act;

(i) Whether Equifax failed to provide at least 12 months of identity protection services free of charge under the Consumer Records Act;

(j) Whether Equifax's actions violated the California Online Privacy Protection Act;

(k) Whether Equifax failed to adequately safeguard PII under the Federal Trade

Commission Act;

(l) Whether Equifax failed to adequately safeguard PII under the Financial Services Modernization Act of 1999, a.k.a. the Gramm-Leach-Bliley Act;

(m) Whether Equifax has been unjustly enriched by its conduct;

(n) Whether Plaintiff and members of the Class are entitled to equitable and declaratory relief, including injunctive relief, and if so, the nature of such relief.

86. Equifax engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

87. **Typicality.** Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and all members of the Class have been injured by the same wrongful, deceptive, and unlawful practices of Equifax and allege similar or the same legal theories.

88. **Adequacy.** Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately assert and protect the interests of the Classes, and has retained counsel experienced in prosecuting class actions. Plaintiff has no interests adverse to the interests of the members of the Classes. Accordingly, Plaintiff is an adequate representative and will

fairly and adequately protect the interests of the Classes.

89. **Superiority.** Fed. R. Civ. P. 23(b)(3). A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit, because individual litigation of the claims of all Class members is economically unfeasible and procedurally impracticable. While the aggregate damages sustained by Class members are in the millions of dollars, the individual damages incurred by each Class member resulting from Equifax's wrongful conduct, do not warrant the expense of individual lawsuits. The likelihood of individual Class members prosecuting separate claims is remote, and, even if every Class member could afford individual litigation, the court system would be unduly burdened by individual litigation of such cases.

90. The prosecution of separate actions by Class members would create a risk of establishing inconsistent rulings and/or incompatible standards of conduct for Equifax. Additionally, individual actions may be dispositive of the interests of the Class, although certain class members are not parties to such actions.

91. **Injunctive and Declaratory Relief.** Fed. R. Civ. P. 23(b)(2). The conduct of Equifax is generally applicable to the Classes as a whole and Plaintiff seeks equitable remedies with respect to the Classes as a whole. As such, the policies and practices of Equifax make declaratory or equitable relief with respect to the Classes as a whole appropriate.

92. **Issue Certification.** Fed. R. Civ. P. 23(c)(4). In the alternative, the common questions of law and fact, set forth above, are appropriate for issue certification on behalf of the Classes.

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

FIRST CAUSE OF ACTION

Violation of Stored Communications Act ("SCA")

(18 U.S.C. § 2702)

93. Plaintiff brings this cause of action on behalf of herself and members of the Nationwide Class.

94. The Federal Stored Communications Act ("SCA") contains provisions that provide consumers with redress if a company mishandles their electronically stored information. The SCA was designed, in relevant part, "to protect individuals' privacy interests in personal and proprietary information." S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555 at 3557.

95. Section 2702(a)(1) of the SCA provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

96. The SCA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* at § 2510(15).

97. Through its equipment, Equifax provides an “electronic communication service to the public” within the meaning of the SCA because it provides consumers at large with mechanisms that enable them to send or receive wire or electronic communications concerning their private financial information to transaction managers, card companies, or banks. Equifax further enables prospective employers, financial institutions, and other entities to request credit reports on consumers and have them provided via electronic communication. The heart of Equifax’s business is the collection and transmission of sensitive personal data.

98. By failing to take commercially reasonable steps to safeguard sensitive private financial information, even after Equifax was aware that customers’ PII and financial information had been compromised, Equifax knowingly divulged customers’ private financial information that was communicated to financial institutions solely for customers’ payment verification purposes, while in electronic storage in Equifax’s payment system.

99. Section 2702(a)(2)(A) of the SCA provides that “a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of

electronic transmission from), a subscriber or customer of such service." 18 U.S.C. § 2702(a)(2)(A).

100. The SCA defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communication system." 18 U.S.C. § 2711(2).

101. An "electronic communications systems" is defined by the SCA as "any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(4).

102. Equifax provides remote computing services to the public by virtue of its systems for consumer credit and debit card payments, which are used by customers and carried out by means of an electronic communications system, namely the use of wire, electromagnetic, photo-optical or photo-electric facilities for the transmission of wire or electronic communications received from, and on behalf of, the customer concerning customer private financial information.

103. By failing to take commercially reasonable steps to safeguard sensitive private financial information, even after Equifax was aware that customers' PII and financial information had been compromised, Equifax has knowingly divulged customers' private financial information that was carried and maintained on Equifax's remote

computing service solely for the customer's payment verification purposes.

104. Furthermore, Equifax unreasonably delayed in notifying class members of the breach. Equifax's press release indicates it discovered the breach at least as early as July 29, 2017. It did not notify consumers until September 7, 2017. SEC filings show that multiple executives unloaded stock options worth, cumulatively, approximately $2 million between August 1st and 4th. Equifax denies the individuals had knowledge, but a reasonable person would at least consider otherwise.

105. As a result of Equifax's conduct described herein and its violations of Section 2702(a)(1) and (2)(A), Plaintiff and the Class members have suffered injuries, including lost money and the costs associated with the need for vigilant credit monitoring to protect against additional identity theft. Plaintiff and Class members have lost, and will continue to lose, time and money addressing the issues caused by the Equifax's inadequate securing of their PII. Plaintiff, on her own behalf and on behalf of the putative class, seeks an order awarding her and the class the maximum statutory damages available under 18 U.S.C. § 2707 in addition to the cost for 3 years of credit monitoring services.

SECOND CAUSE OF ACTION
Negligence
(On Behalf of the Nationwide Class or, alternatively, the California Class)

106. Equifax owed a duty to Plaintiff and Class members, arising from the sensitivity of the information and the foreseeability of its data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding sensitive PII. This duty included, among other things, designing, maintaining, monitoring, and testing Equifax's security systems, protocols, and practices to ensure that Class members' information was adequately secured from unauthorized access.

107. Equifax owed a duty to Class members to implement intrusion detection processes that would detect a data breach in a timely manner.

108. Equifax owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Class members' PII.

109. Equifax also had independent duties under state and federal law that required it to reasonably safeguard Plaintiff's and Class members' PII and promptly notify them about the Breach.

110. Equifax had a special relationship with Plaintiff and the Class members due to Equifax's role and unique circumstances, which established an independent duty of care. Equifax had the ability and knowledge to protect its systems from attack, and should have had the foresight to adequately protect its system from attack due to

previous breaches of Equifax's systems, and Equifax's own data security products. Equifax's role and unique circumstances required a reallocation of risk.

111. Equifax breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Class members' PII; (b) failing to detect the Breach in a timely manner; (c) failing to disclose that Equifax's data security practices were inadequate to safeguard Class members' PII; and (d) failing to provide adequate and timely notice of the Breach.

112. But for Equifax's breach of its duties, Class members' PII would not have been accessed by unauthorized individuals.

113. Plaintiff and the Class members were foreseeable victims of Equifax's inadequate data security practices. Equifax knew or should have known that a breach of its data security systems would cause damage to Class members.

114. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiff's and Class members' PII.

115. As a result of Equifax's willful failure to prevent the Breach, Plaintiff and Class members suffered injury, which includes, but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Class members also have incurred, and

will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. Plaintiff and Class members have lost and will continue to lose time and money addressing the issues caused by the Equifax's inadequate securing of their PII. In addition, the unauthorized acquisition of Plaintiff's and Class members' PII has also diminished the value of the PII.

116. The damages to Plaintiff and the Class members were a proximate, legal, and reasonably foreseeable result of Equifax's breach of its duties.

117. Therefore, Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Negligence Per Se
(Brought on behalf of the Nationwide Class Only)

118. Under the FCRA, 15 U.S.C. §§ 1681e, Equifax is required to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

119. Equifax failed to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA.

120. Plaintiff and Class members were foreseeable victims of Equifax's violation of

the FCRA. Equifax knew or should have known that a breach of its data security systems would cause damages to Class members.

121. As alleged above, Equifax was required under the Gramm-Leach-Bliley Act ("GLBA") to satisfy certain standards relating to administrative, technical, and physical safeguards: (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. *See* 15 U.S.C. § 6801(b).

122. In order to satisfy its obligations under the GLBA, Equifax was also required to "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.4.

123. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems."

124. Further, when Equifax became aware of "unauthorized access to sensitive customer information," it should have "conduct[ed] a reasonable investigation to promptly determine the likelihood that the information has been or will be misused" and "notif[ied] the affected customer[s] as soon as possible."

125. Equifax violated by GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Equifax's (a) failure to implement and maintain adequate data security practices to safeguard Class members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Equifax's data security practices were inadequate to safeguard Class members' PII.

126. Equifax also violated the GLBA by failing to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." This includes, but is not limited to, Equifax's failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

127. Equifax also violated by the GLBA by failing to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer

information.

128. Plaintiff and Class members were foreseeable victims of Equifax's violation of the GLBA. Equifax knew or should have known that its failure to take reasonable measures to prevent a breach of its data security systems, and failure to timely and adequately notify the appropriate regulatory authorities, law enforcement, and Class members themselves would cause damages to Class members.

129. Equifax's failure to comply with the applicable laws and regulations, including the FCRA and the GLBA, constitutes negligence per se.

130. But for Equifax's violation of the applicable laws and regulations, Class members' PII would not have been accessed by unauthorized individuals.

131. As a result of Equifax's failure to comply with applicable laws and regulations, Plaintiff and Class members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class members must monitor financial accounts and credit histories more closely and frequently to guard against identity theft. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class members' PII has also diminished the value of the PII. Plaintiff and Class

members have lost and will continue to lose time and money addressing the issues caused by the Equifax's inadequate securing of their PII.

132. The damages to Plaintiff and the Class members were a proximate, legal, and reasonably foreseeable result of Equifax's breaches of the applicable laws and regulations.

133. Therefore, Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

CLAIMS ON BEHALF OF THE CALIFORNIA CLASS ONLY

FOURTH CAUSE OF ACTION

Unfair Business Practices in Violation of Unfair Competition Law ("UCL")

(Cal. Bus. & Prof. Code § 17200 *et seq*.)

134. Plaintiff bring this cause of action on behalf of herself and the Class members of the California Subclass.

135. The UCL defines unfair business competition to include any "unlawful, unfair or fraudulent" act or practice.

136. During the relevant time period, Equifax engaged in unfair business practices, as described herein, including failing to implement and maintain adequate data security practices to safeguard Class members' PII; failing to detect the Breach in a timely manner; failing to disclose that Equifax's data security practices were inadequate to safeguard Class members' PII; failing to provide adequate and timely notice of the Breach; violating the Fair Credit Reporting Act; violating the Stored

Communications Act; violating the California Consumer Records Act; violating the California Online Privacy Protection Act; failing to safeguard PII adequately under the Federal Trade Commission Act; failing to safeguard PII adequately under the GLBA; among others.

137. During the relevant time period, Equifax also engaged in unfair business practices by omitting material facts it was obligated to or should have disclosed, as alleged herein, including that it knew there was a data breach that affected the PII of over 140 million United States residents, including their Social Security numbers. Equifax’s failure to timely disclose this information has caused substantial injury, with no benefit other than to Equifax.

138. Equifax’s practices, as described herein, constitute unfair business practices in violation of the UCL because, among other things, they are immoral, unethical, unscrupulous, or substantially injurious to consumers and/or any utility of such practices is outweighed by the harm caused to consumers. Equifax’s practices caused substantial injury to Plaintiff and the Class members and are not outweighed by any benefits, and Plaintiff and the Class members could not have reasonably avoided the injuries.

139. As a result of Equifax’s unfair business practices, Plaintiff has suffered injury in fact as alleged herein, which she would not otherwise have suffered but for Equifax’s

conduct. Plaintiff and Class members have lost and will continue to lose time and money addressing the issues caused by the Equifax's inadequate securing of their PII.

140. Pursuant to Business and Professions Code §17204, Plaintiff and Class members are entitled to an order of this Court enjoining such conduct on the part of Equifax, and any other orders and judgments that may be necessary to provide for complete equitable monetary relief by disgorging Equifax's ill-gotten gains, including the monies Equifax received or saved as a result of its wrongful acts and practices detailed herein, and ordering the payment of full restitution. Otherwise, Plaintiff and Class members, and members of the general public, may be irreparably harmed or denied an effective and complete remedy.

141. Additionally, pursuant to Business and Professions Code §17203, Plaintiff and Class members seek an order requiring Equifax to immediately cease such unfair business practices.

FIFTH CAUSE OF ACTION
Unlawful Business Practices in Violation of Unfair Competition Law ("UCL")
(Cal. Bus. & Prof. Code § 17200 *et seq.*)

142. Plaintiff brings this cause of action on behalf of herself and the members of the Class.

143. A business act or practice is "unlawful" under the UCL if it violates any other law or regulation.

144. Equifax's business practices and acts, as described herein, violated and continue to violate, *inter alia*, the Fair Credit Reporting Act, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801 *et seq.*, the California Consumer Records' Act, Cal. Civ. Code § 1798.80 *et seq.*, the California Online Privacy Protection Act, Cal. Bus. & Prof. Code § 22575 *et seq.*, the Federal Trade Commission Act, 15 U.S.C. § 45 *et seq.*, and the Stored Communications Act, 18 U.S.C. § 2702 *et seq.*

145. Plaintiff reserves the right to identify other violations of law as the facts develop.

146. As a result of Equifax's unlawful business practices, Plaintiff has suffered injury in fact as alleged herein, which she would not otherwise have suffered but for Equifax's conduct. Plaintiff and Class members have lost and will continue to lose time and money addressing the issues caused by the Equifax's inadequate securing of their PII.

147. Pursuant to Business and Professions Code §17204, Plaintiff and Class members are entitled to an order of this Court enjoining such conduct on the part of Equifax, and any other orders and judgments that may be necessary to provide for complete equitable monetary relief by disgorging Equifax's ill-gotten gains, including the monies Equifax received or saved as a result of its wrongful acts and practices detailed herein, and ordering the payment of full restitution. Otherwise, Plaintiff,

Class members, and members of the general public may be irreparably harmed or denied an effective and complete remedy.

148. Additionally, pursuant to Business and Professions Code §17203, Plaintiff and the Class seek an order requiring Equifax to immediately cease such unlawful business practices.

SIXTH CAUSE OF ACTION
Violation of the California Consumer Records Act
(Cal. Civ. Code § 1798.80 *et seq.*)

149. Plaintiff brings this cause of action on behalf of herself and the members of the California Subclass.

150. Equifax owns, maintains, and licenses personal information, within the meaning of § 1798.81.5, about Plaintiff and the California Subclass.

151. As a direct and proximate result of Equifax's violations of section 1798.81.5 of the California Civil Code, the Breach described herein occurred.

152. In addition, California Civil Code § 1798.82(a) provides that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be

made in the most expedient time possible and without unreasonable delay . . ."

153. Section 1798.2(b) provides that "[a] person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

154. In the alternative, Equifax maintained computerized data that includes personal information that Equifax does not own as defined by Cal. Civ. Code § 1798.80 *et seq*.

155. Plaintiff and the California Subclass members' PII (including but not limited to names, addresses, and Social Security numbers) includes personal information covered by Cal. Civ. Code § 1798.81.5(d)(1).

156. Because Equifax reasonably believed that Plaintiff and the California Subclass members' personal information was acquired by unauthorized persons during the Breach, it had an obligation to disclose the Breach in a timely and accurate fashion under Cal. Civ. Code § 1798.82(a), or in the alternative, under Cal. Civ. Code § 1798.82(b).

157. Equifax unreasonably delayed notifying affected consumers and the California Attorney General about the Breach. In the interim between Equifax's alleged discovery of the Breach and its public disclosure on September 7, 2017, multiple

Equifax executives sold, cumulatively, approximately $2 million worth of stock options. While Equifax denies that these individuals had knowledge of the Breach, a reasonable inference is that Equifax or Equifax executives chose to delay public notification so that they could profit before the inevitable stock price slump that would follow once the Breach made the news.

158. At this time, no data breach notification fully compliant with Cal. Civ. Code § 1798.82 appears on the California Attorney General's data breach notification website.

159. By failing to disclose the Breach in a timely and accurate manner, Equifax violated Cal. Civ. Code § 1798.82.

160. As a direct and proximate result of Equifax's violations of sections 1798.81.5 and 1798.82 of the California Civil Code, Plaintiff and the California Subclass Members suffered the damages described above, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII. Plaintiff and Class members have lost and will continue to lose time and money addressing the issues caused by the Equifax's inadequate securing of their PII.

161. Plaintiff and the California Subclass seek relief under Civ. Code § 1798.84, including, but not limited to, actual damages in an amount to be proven at trial, and

injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the members of the Class, prays for relief as follows:

1. An Order certifying that this action may be maintained as a Class Action, appointing Plaintiff to represent the proposed Class pursuant to Fed. R. Civ. P. 23(a) and designating her counsel as Class Counsel;
2. An Order enjoining Equifax from future violations of the UCL as alleged herein;
3. A Declaration that Equifax's actions are unlawful as alleged herein;
4. An Order awarding restitution and/or disgorgement of Equifax's profits from its unfair and unlawful practices described herein;
5. An Order awarding compensatory, statutory, and other damages sustained by Plaintiff and members of the Class;
6. An Order awarding Plaintiff and members of the Class applicable civil penalties;
7. An Order awarding Plaintiff attorneys' fees, expert witness fees and other costs;
8. An Order awarding pre-judgment and post-judgment interest on any amounts

awarded to the extent allowed by law; and

9. Such other relief as the Court deems proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and members of the Classes, hereby demands trial by jury as to all matters so triable.

Respectfully submitted, this 29th day of September, 2017.

CONLEY GRIGGS PARTIN LLP

/s/ *Ranse M. Partin*
RANSE M. PARTIN
Georgia Bar No. 556260

4200 Northside Parkway, NW
Building One, Suite 300
Atlanta, Georgia 30327
(404) 467-1155
ranse@conleygriggs.com

Pro Hac Vice Admission Pending:
ZAVERI TABB, APC
DEVAL R. ZAVERI
402 West Broadway
Suite 1950
San Diego, California 92101
(619) 831-6988
dev@zaveritabb.com

ATTORNEYS FOR PLAINTIFF AND THE CLASSES